No. 18-481

IN THE
Supreme Court of the United States

FOOD MARKETING INSTITUTE,
Petitioner,

v.

ARGUS LEADER MEDIA, D/B/A ARGUS LEADER,
Respondent.

On Writ of Certiorari to the
United States Court of Appeals for the Eighth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND TWENTY LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF RESPONDENT

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
ENID ZHOU
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

March 25, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 5

ARGUMENT 6

I. The objective definition of "confidential" commercial information established in *National Parks* is necessary to ensure oversight of government programs that implicate privacy 9

A. Public access to business records promotes accountability of government agencies responsible for enforcement 11

B. Public access to technical specifications and other records from government contractors enables oversight of data collection programs. 19

II. The Government's argument that there is no Article III standing issue in this case is inconsistent with the Court's recent decision in *Frank v. Gaos*. 24

CONCLUSION 28

TABLE OF AUTHORITIES

CASES

9 to 5 Org. for Women Office Workers v. Bd. of Governors of Fed. Reserve Sys., 721 F.2d 1 (1st Cir. 1983) 8

Buckley v. Valeo, 424 U.S. 1 (1976) 10

Critical Mass Energy Project v. NRC, 975 F.2d 871 (D.C. Cir. 1992) (Ginsberg, J., dissenting) 8

DaimlerChrysler Corp v. Cuno, 547 U.S. 332 (2006) 9, 24

Dep't of Air Force v. Rose, 425 U.S. 352 (1976) 7

Dep't of State v. Ray, 502 U.S. 164 (1991) 7

EPA v. Mink, 410 U.S. 73 (1973) 5

Frank v. Gaos, 584 U.S. ___ (2019) 6, 9, 24, 25, 26, 27

Gaos v. Google, Inc., No. 10-4809, 2012 WL 1094646 (N.D. Cal., Mar. 29, 2012) 25

King v. Burwell, 135 S. Ct. 2480 (2015) (Scalia, J., dissenting) 27

Milner v. Dep't of Navy, 562 U.S. 562 (2011) 7

Nat'l Archives & Record Admin. v. Favish, 541 U.S. 157 (2004) 5

Nat'l Parks & Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974) 7

Spokeo v. Robins,
136 S. Ct. 1540 (2016) 26

STATUTES

49 U.S.C. § 44901(l)(2)(B) 23

OTHER AUTHORITIES

155 Cong. Rec. D644 (daily ed. Jun. 4, 2009) 21

156 Cong. Rec. E1,238-E1,239 (daily ed. Jun. 30, 2010) 22

Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe? Hearing Before the Subcomm. on Transportation Sec. & Infrastructure Protection of the H. Comm. on Homeland Sec., 111th Cong. 67 (Mar. 17, 2010) (joint prepared statement of Marc Rotenberg & Lillie Coney) 21, 22

Bart Jansen, *TSA Dumps Near-Naked Rapiscan Body Scanners*, USA Today (Jan. 18, 2013). 23

Brief for the United States as Amicus Curiae 13, *Frank v. Gaos*, 584 U.S. __ (2019) (No. 17-961) 26

Class Respondents' Supplemental Brief on Article III Standing, *Frank v. Gaos*, 584 U.S. __ (2019) (No. 17-961) 26

Complaint, *EPIC v. FTC*, No. 18-942 (D.D.C. filed Apr. 20, 2018) 15

Craig Timberg, *Army Now Says It Won't Put Cameras on Surveillance Aircraft in Maryland*, Wash. Post (Sept. 3, 2014) 24

David G. Savage, *The Fight Against Full-body Scanners at Airports*, L.A. Times (Jan. 13, 2010) 22

David Kravets, *An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle*, Wired (May 2, 2012) 14

Dep't of Homeland Sec., *Privacy Impact Assessment Update for TSA Whole Body Imaging*, 8 (Jul. 23, 2009) 21

EPIC, *Echometrix* (2015) 18

EPIC, *EPIC FOIA – US Drones Intercept Electronic Communications and Identify Human Targets* (Feb. 28, 2013) 23

EPIC, *EPIC FOIA Case – Army Blimps over Washington Loaded with Surveillance Gear, Cost $1.6 Billion* (Aug. 29, 2014) 23

EPIC, *EPIC FOIA Uncovers Google's Privacy Assessment* (Sept. 28, 2012) 12

EPIC, *EPIC v. Education Department – Private Debt Collector Privacy Act Compliance* (2019 19

EPIC, *EPIC v. Education Department: FOIA Documents* (2019) 19

EPIC, *EPIC v. FTC (Facebook Assessments)* (2019) 15

EPIC, *In re Facebook* (2019) 14

EPIC, *Investigations of Google Street View* (2019) 13

EPIC, *Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening)* (2019) 20

Fed. Commc'ns Comm'n, *In the Matter of Google Inc.*, DA 12-592, 27 FCC Rcd. 4012 (2012). 13

Fed. Trade Comm'n, *In the Matter of Google Inc.*, DA 12-592, Notice of Apparent Liability of Forfeiture *Unredacted* (April 13, 2012) 13

FOIA request from EPIC to Army and Air Force Exchange Serv. (Oct. 20, 2009) 17

FOIA Request from EPIC to Dep't of Homeland Sec. (Apr. 14, 2009) 21

FOIA Request from EPIC to Fed. Trade Comm'n (Mar. 20, 2018) 15

H.R. Rep. No. 95–1382 (1978) 8

In re Echometrix (Complaint, Request for Investigation, Injunction, and Other Relief) (Sept. 25, 2009) 17

Jeanne Meserve & Mike M. Ahlers, *Body scanners can store, send images, group says*, CNN (Jan. 11, 2010) 22

Joe Sharkey, *Whole-Body Scans Pass First Airport Tests*, N.Y. Times (Apr. 6, 2009) 20

Letter from James Madison to W.T. Barry (Aug. 4, 1822) 6

Letter from Michael Richter, Chief Privacy Officer, Product, Facebook and Erin Egan, Chief Privacy Officer, Policy, Facebook to James A. Kohm, Esq., Associate Dir. For the Division of Enforcement, Bureau of Consumer Protection, Fed. Trade Comm'n (Apr. 23, 2013) 15

Letter from Teresa Z. Cavanaugh, Chief, Investigations and Hearings Division Enforcement Bureau, Fed. Commc'ns Comm'n, to Google 2 (April 13, 2012) 13

Louis Brandeis, *Other People's Money* (1933) 10

Lucia Mutikani, *Google Fined $25,000 for Impeding FCC Investigation*, Reuters (Apr. 15, 2012) 13

Matthew L. Wald, *Mixed Signals on Airport Scanners*, N.Y. Times (Jan. 12, 2009) 22

Mya Frazier, *Big Tech's Bid to Control FOIA*, Colum. Journalism Rev. (Feb. 2, 2018) 10

Nancy Gohring, *Google Kills Buzz*, Computerworld (Oct. 14, 2011) 12

Order, *Frank v. Gaos*, 586 U.S. ___ (Nov. 20, 2018) (No. 17-961) 26

Paul Giblin & Eric Lipton, *New Airport X-Ray Scans Bodies, Not Just Bags*, N.Y. Times (Feb 24, 2007) 20

Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011) 14

Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011) 12

Press Release, Fed. Trade Comm'n, FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers (Nov. 30, 2010). 18

Press Release, Fed. Trade Comm'n, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018) 17

Reprocessed Independent Assessor's Report on Facebook's Privacy Program: For the Period August 15, 2012 to February 11, 2013, PricewaterhouseCoopers (June 26, 2018).....16

S. Rep. No. 89-813 (1965).....6, 7

Supplemental Brief for the United States As Amicus Curiae Supporting Neither Party, *Frank v. Gaos*, 584 U.S. __ (2019) (No. 17-961) 26

Transp. Sec. Admin., *Whole-Body Imaging* (May 28, 2009) 21

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues, to promote government transparency, and to protect privacy, the First Amendment, and other constitutional values.

EPIC has filed several briefs before this Court and other federal courts concerning the federal Freedom of Information Act. *See, e.g.*, Brief of *Amici Curiae* EPIC et al., *FCC v. AT&T*, 562 U. S. 397 (2011) (No. 09-1279) (arguing that the phrase "personal privacy" in the FOIA applies to individuals, not corporations); Brief of *Amici Curiae* EPIC et al., *ATF v. City of Chicago*, 537 U.S. 1229 (2003) (02-322) (arguing that FOIA procedures should be updated "in an age of electronic record keeping"); Brief of *Amici Curiae* EPIC et al., *N.Y. Times v. DOJ*, 756 F.3d 100 (2d Cir. 2014) (No. 13-422) (arguing that OLC opinions should be disclosed under FOIA).

EPIC is also one of the top FOIA litigators in the United States. FOIA Project, *FOIA Suits Filed by Nonprofit/Advocacy Groups Have Doubled Under Trump* (Oct. 18, 2018).[2] EPIC relies upon access to

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

[2] EPIC is among the top five FOIA litigators in the United States for the period 2001-2018, as measured by the

government documents to pursue its mission: to focus public attention on emerging privacy and civil liberties issues. Many of EPIC's government transparency projects have depended on access to commercial information contained in agency documents. *See, e.g.*, EPIC, *EPIC v. FTC (Facebook Assessments)* (2019);[3] EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones* (2019);[4] EPIC, *EPIC v. Education Department – Private Debt Collector Privacy Act Compliance* (2019);[5] EPIC, *EPIC v. DHS – Body Scanner Complaints* (2019).[6] The documents EPIC obtains through its FOIA work are reported in the national media. *See, e.g.*, Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show*, Buzzfeed (Mar. 11, 2019);[7] Ava Kofman, *The FBI is Building a National Watchlist that Gives Companies Real-Time Updates on Employees*, The Intercept (Feb. 4, 2017);[8] Spencer Woodman, *Documents Suggest Palantir Could Help Power Trump's 'Extreme Vetting' of Immigrants*, The Verge (Dec. 21, 2016);[9] Charlie

---

number of cases filed. http://foiaproject.org/2018/10/18/nonprofit-advocacy-groups-foia-suits-double-under-trump/.

[3] https://epic.org/foia/ftc/facebook/.

[4] https://epic.org/privacy/drones/.

[5] https://epic.org/foia/ed/.

[6] https://epic.org/foia/dhs/bodyscanner/complaints/.

[7] https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.

[8] https://theintercept.com/2017/02/04/the-fbi-is-building-a-national-watchlist-that-gives-companies-real-time-updates-on-employees/.

[9] https://www.theverge.com/2016/12/21/14012534/palantir-peter-thiel-trump-immigrant-extreme-vetting.

Savage, *Facial Scanning is Making Gains in Surveillance*, N.Y. Times (Aug. 21, 2013).[10]

EPIC's brief is joined by the following distinguished experts in law, technology, and public policy.

Legal Scholars and Technical Experts

Alessandro Acquisti
Professor, Carnegie Mellon University

Anita L. Allen
Henry R. Silverman Professor of Law and Philosophy, Vice Provost, University of Pennsylvania Law School

Danielle Keats Citron
Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law

Simon Davies
Publisher, the Privacy Surgeon, Fellow of the University of Amsterdam,
Founder of Privacy International and EPIC Senior Fellow

Addison Fischer
Founder and Chairman, Fischer International Corp.

Hon. David Flaherty
Former Information and Privacy Commissioner for British Columbia

Lorraine G. Kisselburgh
Assistant Professor, Purdue University

Chris Larsen
Executive Chairman, Ripple Inc.

---

[10] https://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Roger McNamee
Elevation Partners

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Dr. Peter G. Neumann
Chief Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science

Frank Pasquale
Professor of Law, Univ. of Maryland Francis King Carey School of Law

Deborah C. Peel, M.D.
President of Patient Privacy Rights

Dr. Stephanie Perrin
President, Digital Discretion, Inc.

Bilyana Petkova
EPIC Scholar-in-Residence; Assistant Professor, Maastricht University

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, John A. Paulson School of Engineering and Applied Sciences

Anne L. Washington
Assistant Professor of Data Policy, NYU Steinhardt School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The Freedom of Information Act ("FOIA") establishes a right of the public to know "what their government is up to." *Nat'l Archives & Record Admin. v. Favish*, 541 U.S. 157, 171 (2004). The FOIA is necessary to enable the public to obtain information "from possibly unwilling official hands." *EPA v. Mink*, 410 U.S. 73, 80 (1973). But "official hands" are often not the only hands FOIA requesters must grapple with. Private companies—as government contractors and vendors—play an integral role in government activities that impact the privacy of Americans. And these private parties, acting on behalf of public agencies and with public funding, often hide their activities behind an expansive view of one of the exemptions in the FOIA. Government agencies are also responsible for investigating and enforcing privacy obligations on private companies that concern the privacy rights of Americans. Public access to the commercial information contained in agency records is therefore necessary to ensure adequate oversight of these enforcement duties.

Petitioner's proposal for a broad, subjective interpretation of "confidential" in Exemption 4 would deprive the public, and government watchdogs such as EPIC, of access to important information about "what the government is up to." Under a subjective test, companies could seek to withhold any commercial information that they consider confidential without regard to the public interest in disclosure.

There are also significant jurisdictional questions that make this case a poor vehicle to address the Exemption 4 issue. As the Court recently explained in *Frank v. Gaos*, 584 U.S. ___, 2019 WL 1264582 (Mar.

20, 2019), Article III standing must be analyzed by lower courts in the first instance. Yet the lower courts did not analyze whether the Food Marketing Institute, a trade association, had standing to intervene and appeal the district court judgment. In fact, the Petitioner in this case has a significantly weaker standing claim than the consumer plaintiffs in *Gaos*. The Government's arguments in the two cases are also irreconcilable. The Court should remand for the lower court to address standing.

ARGUMENT

"An informed electorate is vital to the proper operation of a democracy." S. Rep. No. 89-813, 3 (1965). For this reason, Congress passed the Freedom of Information Act ("FOIA") in 1966. Senator Long quoted James Madison as he introduced the bill:

> A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own governors, must arm themselves with the power knowledge gives.

Id. at 2-3 (quoting Letter from James Madison to W.T. Barry (Aug. 4, 1822)).[11]

Congress passed the FOIA to "overhaul the public-disclosure section of the Administrative Procedure Act (APA)" and correct the law's shift to more of "a withholding statute than a disclosure statute." *Milner*

---

[11] *Available at* https://www.loc.gov/resource/mjm.20_0155_0159/?sp=1&st=text.

v. Dep't of Navy, 562 U.S. 562, 565 (2011). Congress intended the FOIA "to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1976). While Congress acknowledged that the public's interest in transparency would, in some circumstances, have to be balanced with competing interests in privacy, Congress envisioned the FOIA as "a workable formula which encompasses, balances, and protects all interests, yet places emphasis on the fullest responsible disclosure." S. Rep. No. 89-813, 3 (1965). Thus, the FOIA creates a "strong presumption in favor of disclosure." *Dep't of State v. Ray*, 502 U.S. 164, 173 (1991), and the FOIA's nine exemptions "must be narrowly construed." *Milner*, 562 U.S. at 565.

Nearly thirty-five years ago, the D.C. Circuit adopted the substantial competitive harm test to determine the scope of "confidential" commercial information protected by Exemption 4. *Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974). The court rejected the same subjective test advanced by Petitioners. *Id.* at 766. The First Circuit, in adopting *National Parks*, quoted the House Committee on Government Operations in its 1978 Report to similar effect:

> disclosure policy cannot be contingent on the subjective intent of those who submit information. For example, it clearly would be inappropriate to withhold all information, no matter how innocuous, submitted by a corporation with a blanket policy of refusing all public requests for information.

9 to 5 Org. for Women Office Workers v. Bd. of Governors of Fed. Reserve Sys., 721 F.2d 1, 9 (1st Cir. 1983) (quoting H.R. Rep. No. 95–1382, 18 (1978)). When the D.C. Circuit in *Critical Mass* adopted a subjective test for a limited subset of records (information given voluntarily to government agencies), then-Judge Ginsburg warned of the perils of allowing such a test:

> No longer is there to be an independent judicial check on the reasonableness of the provider's custom and the consonance of that custom with the purposes of exemption 4 and of the Act of which the exemption is part. To the extent that the court allows providers to render categories of information confidential merely by withholding them from the public long enough to show a custom, the revised test is fairly typed "subjective" . . .

Critical Mass Energy Project v. NRC, 975 F.2d 871, 885 (D.C. Cir. 1992) (en banc) (Ginsberg, J., dissenting).

A broad, subjective definition of "confidential" would limit the public's ability to conduct meaningful oversight of government surveillance activities and the government's enforcement of privacy obligations on commercial entities. The Government now routinely relies on contractors to develop and deploy systems used to collect personal data and to conduct surveillance. And regulatory agencies gather commercial information from businesses to enforce federal privacy laws. A subjective confidentiality test under Exemption 4 would allow companies, acting with taxpayer dollars on behalf of federal agencies, to conceal

information that would otherwise be available to the public.

There is also significant doubt that the Petitioner has satisfied the standing requirements of Article III necessary to invoke this Court's jurisdiction. *See* Resp't Br. 1. As in *Frank v. Gaos*, 584 U.S. ___, 2019 WL 1264582 (Mar. 20, 2019), the Court has "an obligation to assure [itself] of litigants' standing under Article III." Slip op. 5 (quoting *DaimlerChrysler Corp v. Cuno*, 547 U.S. 332, 340 (2006)). The Petitioner's standing claim here is much weaker than the unlawful disclosure injury that the plaintiffs alleged in *Gaos*. The records at issue in this case were not even created by the Food Marketing Institute, and the Institute was not the entity that provided data to the USDA.

The Court in *Gaos* found remand was necessary because the lower courts must address standing in the first instance, and this case should be no different.

I. The objective definition of "confidential" commercial information established in *National Parks* is necessary to ensure oversight of government programs that implicate privacy.

The public must have access to commercial information in agency records to conduct effective oversight of government programs that implicate privacy. Federal agencies, across the government, contract with private companies to build data collection and surveillance systems. Technical specifications, contracts, and other similar records describing the functions of these systems is provided to the Government by private companies. These records include commercial information that should be available to the public. Without access to this information, it would be

impossible to verify whether the systems do what the government says they do, or whether the systems pose a threat to the privacy of Americans. The government also obtains commercial information from companies during the course of investigating potential privacy violations. Access to commercial information held by agencies is thus also necessary for the public to evaluate the government's protection of privacy rights.

Companies that build data collection systems are notoriously secretive. For example, Amazon and Facebook have requested state and local governments alert them of open government requests concerning their business practices immediately upon receipt. Mya Frazier, *Big Tech's Bid to Control FOIA*, Colum. Journalism Rev. (Feb. 2, 2018).[12] Many companies do not want their work on government surveillance programs to be revealed.

But "[s]unlight is said to be the best of disinfectants." *Buckley v. Valeo*, 424 U.S. 1, 67 (1976) (quoting Louis Brandeis, *Other People's Money* 62 (1933)). And for watchdog groups such as EPIC, access to agency records, including commercial information provided by contractors and vendors, is essential to understand the privacy implications of government activities. A broad, subjective definition of "confidential" in Exemption 4 would limit public oversight of the programs of federal agencies.

---

[12] https://www.cjr.org/business_of_news/facebook-amazon-foia.php.

A. Public access to business records promotes accountability of government agencies responsible for enforcement.

Government agencies, including the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC"), are charged with investigating business practices that may violate the privacy rights of consumers. But oversight does not end with federal agencies. EPIC and other watchdog organizations rely on the FOIA to inform the public about emerging privacy issues and to independently assess the risks these programs pose. Public oversight of the functions of government—the purpose of the FOIA—is not possible if the technical details and other commercial information collected by federal agencies is not accessible to the public.

The FOIA enables public oversight of agencies' and businesses' compliance with privacy laws in several ways. First, records from enforcement agencies, such as the FTC and FCC, can inform the public about whether companies are engaged in business practices that threaten consumer privacy. These records contain commercial information gathered during investigations and pursuant to consent decrees. Second, agencies compile technical specifications and other information that contain commercial information about the contractors that build and operate government systems. These records can have implications for oversight of both government data collection and of consumer privacy investigations. Businesses typically seek to withhold this information from the public.

Commercial information EPIC obtained as a result of FOIA requests submitted to the FTC, the FCC, and the DOJ has helped improve the effectiveness of

these agencies and safeguarded the America public. For example, EPIC was able to obtain information about Google's privacy practices from the FTC in 2012. EPIC, *EPIC FOIA Uncovers Google's Privacy Assessment* (Sept. 28, 2012).[13] Google entered into a consent decree with the FTC in 2010 after it violated users' privacy by disclosing their private contact lists. *See* EPIC, *In re Google Buzz* (2019). As part of the settlement, the FTC required Google to file regular privacy assessment reports with the Commission detailing its steps to comply with the consent order. Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011).[14] Google shuttered Buzz after the FTC investigation. Nancy Gohring, *Google Kills Buzz*, Computerworld (Oct. 14, 2011).[15] The release of Google's privacy assessments gave the public greater insight into the company's privacy practices and facilitated future enforcement efforts.

In another case, EPIC's FOIA work led to the disclosure of records that made clear the full extent of Google's unlawful collection of private Wi-Fi data. Google was subject to numerous investigations after it was revealed that the company had collected private Wi-Fi data via its "Street View" vehicles. EPIC,

---

[13] https://epic.org/2012/09/epic-foia-uncovers-googles-pri.html.

[14] https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

[15] https://www.computerworld.com/article/2499002/google-kills-buzz.html.

Investigations of Google Street View (2019).[16] EPIC and others wrote to the FCC to urge an investigation; the Commission ultimately fined Google a mere $25,000 for obstructing the investigation. Lucia Mutikani, *Google Fined $25,000 for Impeding FCC Investigation*, Reuters (Apr. 15, 2012).[17] The FCC initially released only a heavily redacted version of its report on the investigation. Fed. Commc'ns Comm'n, *In the Matter of Google Inc.*, DA 12-592, 27 FCC Rcd. 4012 (2012). EPIC subsequently filed several FOIA requests seeking disclosure of the full, unredacted report, and disclosure of records from the related Justice Department investigation. EPIC, *Investigations of Google Street View*, *supra*. In response to the FOIA requests, the FCC released a letter it had sent to Google rejecting the company's "very broad request for confidential treatment of the information it submitted" in response to the Commission's investigatory inquiry. Letter from Teresa Z. Cavanaugh, Chief, Investigations and Hearings Division Enforcement Bureau, Fed. Commc'ns Comm'n, to Google 2 (April 13, 2012).[18] On April 28, 2012, Google released a complete, unredacted copy of the FCC's report. Fed. Trade Comm'n, *In the Matter of Google Inc.*, DA 12-592, Notice of Apparent Liability of Forfeiture *Unredacted* (April 13, 2012).[19] Significantly, the full report made clear that

---

[16] https://epic.org/privacy/streetview/.

[17] https://www.reuters.com/article/net-us-google-fine/google-fined-25000-for-impeding-fcc-investigation-idUSBRE83F00Q20120416.

[18] https://transition.fcc.gov/foia/Letter-Ruling-Regarding-Confidentiality-Request.pdf.

[19] *Available at* https://assets.documentcloud.org/documents/351298/fcc-report-on-googles-street-view.pdf.

Google had intentionally intercepted payload data for business purposes and that many supervisors and engineers within the company reviewed the code and the design documents associated with the project. *See* David Kravets, *An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle*, Wired (May 2, 2012).[20]

Records EPIC obtained from the FTC under the FOIA also raised important questions about whether the agency has pursued effective oversight of companies subject to its legal authorities. In 2011 the FTC opened an investigation into Facebook's privacy practices and subsequently entered into a consent decree requiring the company to implement a comprehensive privacy program and submit to third-party audits for 20 years. *See* EPIC, *In re Facebook* (2019);[21] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011).[22] Under the terms of the order, Facebook is required to submit the independent audits to the FTC, but the FOIA is currently the only mechanism that ensures those audits will be made public. In the wake of the Cambridge Analytica scandal, EPIC filed a FOIA request to the FTC seeking documents related to the enforcement of the consent order, including the full release of all Facebook privacy assessments. *See* FOIA Request from

---

[20] https://www.wired.com/2012/05/google-wifi-fcc-investigation/.

[21] https://epic.org/privacy/inrefacebook/.

[22] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

EPIC to Fed. Trade Comm'n (Mar. 20, 2018).[23] EPIC eventually sued the FTC for the release of these documents. Complaint, *EPIC v. FTC*, No. 18-942 (D.D.C. filed Apr. 20, 2018).

As a result of EPIC's lawsuit, the FTC has released partially redacted versions of Facebook's privacy assessments and hundreds of pages of communications between the Commission and Facebook. The communications show that when Facebook initially submitted its first privacy assessment in 2013, the company enclosed two versions of the privacy assessment—a confidential version and a non-confidential version with self-selected redactions. *See* EPIC, *EPIC v. FTC (Facebook Assessments)* (2019).[24] Facebook's non-confidential version submitted to the FTC liberally applied redactions, yet the FTC reprocessed this assessment in the course of EPIC's lawsuit and released much of the information that Facebook had originally claimed was "confidential." *See, e.g.*, Letter from Michael Richter, Chief Privacy Officer, Product, Facebook and Erin Egan, Chief Privacy Officer, Policy, Facebook to James A. Kohm, Esq., Associate Dir. For the Division of Enforcement, Bureau of Consumer Protection, Fed. Trade Comm'n (Apr. 23, 2013);[25] *cf.* Independent Assessor's Report on Facebook's Privacy Program: For the Period August 15, 2012 to February 11,

---

[23] https://www.epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20180320-Request.pdf.

[24] https://epic.org/foia/FTC/facebook/.

[25] *Available at* https://epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20181012-FTC-FB-Communications.pdf (page 19).

2013, PricewaterhouseCoopers (reprocessed version released June 26, 2018).[26]

The FTC's use of the D.C. Circuit's *National Parks* test to reprocess the privacy assessments shows that much of what Facebook had considered "confidential" was often inconsequential and would not cause substantial competitive harm if released to the public.

Without the full release of these assessments, the public would be left in the dark about the effectiveness of third-party audits. In the 2017 privacy assessment, which included the period when Facebook knew of Cambridge Analytica's illicit data transfer, the auditor erroneously certified that the privacy controls were operating with "sufficient effectiveness." In fact, Facebook knew about the significant breach of persona data and never informed the FTC. None of the documents released under the FOIA indicate that Facebook notified the Commission of its knowledge that Cambridge Analytica unlawfully harvested the data of millions of Facebook users. While the FTC reprocessed EPIC's FOIA requests for the privacy assessments and released more information, significant sections of the assessments are redacted under Exemption 4. In the aftermath of the Cambridge Analytica scandal, three years after Facebook discovered the unlawful data transfer, the FTC launched an open investigation into Facebook's privacy practices. Press Release, Fed. Trade Comm'n, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding

---

[26] https://www.epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20180626-FB-Assessment-2013.pdf.

Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018).[27]

In other instance, the release of records, containing commercial, under the FOIA have led to significant changes in agency practices and helped safeguard American military families. For example, in 2009, EPIC filed a FOIA request to the Army and Air Force Exchange Service seeking agency records about the software program "My Military Sentry," including any contracts between the agency and Echometrix, Inc. FOIA request from EPIC to Army and Air Force Exchange Serv. (Oct. 20, 2009).[28] Echometrix produced parental control software and promised to monitor children's online activity. But Echometrix also collected data about children and sold the data to third parties for market-intelligence research.

EPIC filed a complaint with the FTC in 2009 alleging that Echometric had engaged in unfair and deceptive trade practices by representing that its software protects children while simultaneously collecting and disclosing information about children's online activity—a direct violation of the Children's Online Privacy Protection Act. *In re Echometrix* (Complaint, Request for Investigation, Injunction, and Other Relief) (Sept. 25, 2009).[29] EPIC obtained documents as a result of its FOIA request that revealed the Defense Department canceled a contract with Echometrix

---

[27] https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[28] https://epic.org/privacy/echometrix/AAFES_FOIA.PDF.

[29] http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.

following an EPIC complaint to the FTC in 2009. *See* EPIC, *Echometrix* (2015).[30]

As a consequence of EPIC's FOIA work, the Army and Air Force Exchange Service removed My Military Sentry from their online store, stating in an e-mail to Echnometrix, "[t]he collection of AAFES customer information (personal or otherwise) for any other purpose than to provide quality customer service is prohibited . . . . Giving our customers the ability to opt out does not address this issue." *Id.*

The FTC also took action against the firm, based on EPIC's FOIA work. The Commission eventually announced a settlement of its charge against Echometrix requiring the company to not use or share information obtained through its programs for any purpose other than allowing registered users to use their account; destroy the information illicitly transferred to third-party marketers; and requires standard report and record-keeping provisions to allow the Commission to monitor compliance. Press Release, Fed. Trade Comm'n, FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers (Nov. 30, 2010).[31] EPIC's access to commercial records helped protect military families and also ensure that FTC pursued its enforcement obligations.

In another case, documents EPIC obtained from the U.S. Department of Education, including

---

[30] https://epic.org/privacy/echometrix/.

[31] https://www.ftc.gov/news-events/press-releases/2010/11/ftc-settles-company-failed-tell-parents-childrens-information.

commercial information, revealed that many private debt collection agencies maintained incomplete and insufficient quality controls for the data they collect. *See* EPIC, *EPIC v. Education Department – Private Debt Collector Privacy Act Compliance* (2019).[32] As government contractors, debt collectors must follow the Privacy Act, a federal law that protects personal information. The Department of Education also requires student debt collectors to submit quality control reports indicating whether the companies maintain accurate student loan information. The documents obtained by EPIC revealed that many companies provided small sample sizes to conceal possible violations of the Act. *See* EPIC, *EPIC v. Education Department: FOIA Documents* (2019).[33] The documents also showed that many companies did not submit required information about Privacy Act compliance to the Department of Education. EPIC's pursuit of the release of this information allowed for greater public oversight of the Department of Education in overseeing Privacy Act compliance with private debt collectors.

B. Public access to technical specifications and other records from government contractors enables oversight of data collection programs.

Public oversight of government data collection and surveillance systems also requires access to the contracts and technical specification records that private manufacturers provide the government. Substantial privacy problems that led to bipartisan reform would not have been uncovered if EPIC and others

---

[32] https://epic.org/foia/ed/.

[33] https://epic.org/foia/ed/#foia.

could not obtain and analyze agency records that describe these systems and how they function.

For example, EPIC relied on documents obtained under the FOIA, including commercial information such as technical specifications and contracts, to assess the privacy implications of the Transportation Security Administration's ("TSA") use of body scanners in U.S. airports. *See* EPIC, *Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening)* (2019).[34] The campaign against the deployment of body scanners, which captured nude images of every airline passenger, exemplifies the type of public oversight that would be nearly impossible if Exemption 4 imposed a broad, subjective definition of "confidential." In 2007, the TSA began testing body scanners in select U.S. airports. Paul Giblin & Eric Lipton, *New Airport X-Ray Scans Bodies, Not Just Bags*, N.Y. Times (Feb 24, 2007).[35] The TSA's announcement that it would make the scanners mandatory for primary screening in all U.S. airports was met with swift and bipartisan opposition. Joe Sharkey, *Whole-Body Scans Pass First Airport Tests*, N.Y. Times (Apr. 6, 2009).[36] Republican Congressman Jason Chaffetz introduced an amendment to prohibit the TSA "from using Whole Body-Imaging machines for primary screening at airports," require the TSA "to give passengers the option of a pat-down search in place of going through a WBI machine, information on the images generated by the WBI, the privacy policies in place, and the right to request a pat-

---

[34] https://epic.org/privacy/airtravel/backscatter/.

[35] https://www.nytimes.com/2007/02/24/us/24scan.html.

[36] https://www.nytimes.com/2009/04/07/business/07road.html.

down search," and prohibit the TSA "from storing, transferring, or copying the images " 155 Cong. Rec. D644 (daily ed. Jun. 4, 2009). The amendment passed 310-118. *Id.*

In the midst of this public debate, EPIC filed a FOIA request with the Department of Homeland Security ("DHS") for documents regarding the procurement and use of the body scanners. FOIA Request from EPIC to Dep't of Homeland Sec. (Apr. 14, 2009)[37]. As a result of EPIC's FOIA suit, the agency released device specifications, including procurement documents and contracts with L3 and Rapiscan Systems, that showed that the scanners were able to store and transfer images. *Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe? Hearing Before the Subcomm. on Transportation Sec. & Infrastructure Protection of the H. Comm. on Homeland Sec.*, 111th Cong. 67 (Mar. 17, 2010) (joint prepared statement of Marc Rotenberg & Lillie Coney) (Hereinafter "EPIC Body Scanner Testimony").

The documents contradicted the TSA's previous representations that the devices could not store or transmit scans. Dep't of Homeland Sec., *Privacy Impact Assessment Update for TSA Whole Body Imaging*, 8 (Jul. 23, 2009) (TSA had "the manufacturer disable the data storage capabilities prior to delivery to TSA");[38] Transp. Sec. Admin., *Whole-Body Imaging* (May 28, 2009) ("The image cannot be stored, transmitted or printed, and are deleted immediately once viewed. In fact, the machines have zero storage

---

[37] *Available at* https://epic.org/foia/FOIA_041409.pdf.

[38] *Available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf.

capability.")[39] The documents obtained by EPIC also called into question whether the scanners could detect powdered explosives. EPIC Body Scanner Testimony. The story was widely reported and of significant interest to the public. *See, e.g.*, Matthew L. Wald, *Mixed Signals on Airport Scanners*, N.Y. Times (Jan. 12, 2009);[40] Jeanne Meserve & Mike M. Ahlers, *Body scanners can store, send images, group says*, CNN (Jan. 11, 2010).[41] In the immediate aftermath, Rep. Chaffetz remarked, "We don't need to look at naked 8-year-olds and grandmothers to secure airplanes. I think it's a false argument to say we have to give up all of our personal privacy in order to have security." David G. Savage, *The Fight Against Full-body Scanners at Airports*, L.A. Times (Jan. 13, 2010).[42] Rep. Chaffetz later used documents that EPIC received under the FOIA, which included commercial information, to support efforts to limit the use of body scanners in U.S. airports and to enhance the privacy protections for travelers 156 Cong. Rec. E1,238-E1,239 (daily ed. Jun. 30, 2010).[43]

Ultimately, public outcry led Congress to require the TSA to remove all body scanners from U.S. airports that could not be programmed to produce a

---

[39] https://web.archive.org/web/20090528121532/http://www.tsa.gov/approach/tech/body_imaging.shtm.

[40] https://www.nytimes.com/2010/01/13/us/13scanners.html.

[41] http://www.cnn.com/2010/TRAVEL/01/11/body.scanners/.

[42] http://articles.latimes.com/2010/jan/13/nation/la-na-terror-privacy13-2010jan13.

[43] *Available at* https://www.congress.gov/crec/2010/06/30/CREC-2010-06-30-pt1-PgE1238-2.pdf.

generic human outline of a traveler instead of a nude image. 49 U.S.C. § 44901(l)(2)(B). The TSA subsequently removed the backscatter x-ray body scanners manufactured by Rapiscan Systems because the company could not produce the necessary software. Bart Jansen, *TSA Dumps Near-Naked Rapiscan Body Scanners*, USA Today (Jan. 18, 2013).[44]

Many other oversight campaigns have relied on technical data provided to federal agencies and then obtained through the FOIA to reform agency practices. For example, EPIC obtained records from U.S. Customs and Border Protection ("CBP") that included product specifications for drones; these specifications showed that Predator B drones operated by CBP are able to recognize and identify a person on the ground. EPIC, *EPIC FOIA – US Drones Intercept Electronic Communications and Identify Human Targets* (Feb. 28, 2013).[45] An EPIC FOIA also revealed that Army blimps deployed over Washington, D.C., contained extensive surveillance equipment, including video surveillance capabilities. EPIC, *EPIC FOIA Case – Army Blimps over Washington Loaded with Surveillance Gear, Cost $1.6 Billion* (Aug. 29, 2014).[46] After this was revealed, the Army publicly committed not to put cameras on the blimps over the capitol area. Craig Timberg, *Army Now Says It Won't Put Cameras on*

---

[44] https://www.usatoday.com/story/travel/flights/2013/01/18/naked-airport-scanners/1845851/.

[45] https://epic.org/2013/02/epic-foia---us-drones-intercep.html.

[46] https://epic.org/2014/08/epic-foia-case---army-blimps-o.html.

Surveillance Aircraft in Maryland, Wash. Post (Sept. 3, 2014).[47]

* * *

These examples show how public access to commercial information is necessary to enable oversight of government practices that implicate privacy rights. If the *National Parks* standard is diminished, Exemption 4 could prevent the public from accessing this critical information.

II. The Government's argument that there is no Article III standing issue in this case is inconsistent with the Court's recent decision in *Frank v. Gaos*.

There is "a substantial question" about whether Petitioner has standing to appeal the lower court's judgment. The standing issue was not addressed by the lower courts and cannot be resolved by this Court in the first instance. *Frank v. Gaos*, 586 U.S. ___, 2019 WL 1264582, slip op. at 6 (Mar. 20, 2019) ("We 'are a court of review, not of first view.'"). The Court has "an obligation to assure [itself] of litigants' standing under Article III." *Id.* at 5 (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 340 (2006). Yet the United States simply asserts that "petitioner had Article III standing to appeal." Br. United States As Amicus Curiae 31 [hereinafter United States *Food Marketing Institute* Amicus]. The Government's assertion in this case is inconsistent with its arguments challenging consumers' standing to sue for privacy violations in *Frank v. Gaos*. The plaintiffs in *Gaos* have a much stronger

---

[47] https://www.washingtonpost.com/news/the-switch/wp/2014/09/03/armys-eyes-in-the-sky-built-to-spot-people-from-5-kilometers-away/.

standing claim than the intervenor-petitioner trade association in this case, and the Court nevertheless remanded *Gaos* to the lower courts to address standing in the first instance.

In *Frank v. Gaos*, the Court granted a Writ of Certiorari to decide "whether a class action settlement that provides a *cy pres* award but no direct relief to class members satisfies the requirement that a settlement binding class members be "fair, reasonable, and adequate."' *Gaos*, 586 U.S., slip op. at 5. The underlying dispute in *Gaos* concerned consolidated class action complaints against Google, alleging that the company violated users' privacy by disclosing their search queries to owners of third-party websites. *Id.* at 2. Google filed several motions to dismiss the complaints, which were granted in part and denied in part. *Id.* at 3. The lower court held, in particular, that one of the plaintiffs had standing to sue for violations of the class members' rights under the Stored Communications Act, 18 U.S.C. § 2702(a). *Gaos v. Google, Inc.*, No. 10-4809, 2012 WL 1094646, *4 (N.D. Cal., Mar. 29, 2012). The plaintiffs later entered into a settlement with Google on behalf of all class members, which "required Google to include certain disclosures about referrer headers on three of its webpages" but allowed Google to "continue its practice of transmitting users' search terms in referrer headers." *Gaos*, 586 U.S., slip op. at 4. The settlement provided no monetary or injunctive relief to class members; several class members challenged the fairness of the settlement. *Id.* at 4.

The standing issue in *Gaos* was not raised by any of the parties during the appeal of the settlement. Indeed, the issue was not raised at all after the settlement until the United States Solicitor General "filed a

brief as *amicus curiae* supporting neither party" on the merits in the Court. *Id.* at 5. The Solicitor General argued that "There is a substantial question about whether plaintiffs had [Article III] standing" to pursue their Stored Communications Act claims. Brief for the United States as Amicus Curiae 13, *Frank v. Gaos*, 584 U.S. __ (2019) (No. 17-961) [hereinafter United States *Gaos* Amicus Brief]. The basis of the Solicitor General's argument was that the district court did not apply the Article III standing test articulated by the Court in *Spokeo v. Robins*, 136 S. Ct. 1540, 1548 (2016). *See* United States *Gaos* Amicus Brief, *supra*, at 13–15.

The Court ordered supplemental briefing on the standing issue after oral argument. Order, *Frank v. Gaos*, 586 U.S. ___ (Nov. 20, 2018) (No. 17-961). And the parties filed extensive briefs on the issue, raising "a wide variety of legal and factual issues not addressed in the merits briefing before [the Court] or at oral argument." *Gaos*, 586 U.S., slip op. at 6. The Class Plaintiffs filed a supplemental brief and explained that "the alleged wrongful disclosure of individual communications supports standing here" and that "centuries of law likewise establish that persons whose *communications* are disclosed without authorization 'need not allege any *additional* harm beyond' the disclosure itself. Class Respondents' Supplemental Brief on Article III Standing 5, *Frank v. Gaos*, 584 U.S. ___ (2019) (No. 17-961) (emphasis in original). The Solicitor General, in contrast, argued that none of the named plaintiffs has Article III standing to challenge the unlawful disclosure of their private communications. Supplemental Brief for the United States As Amicus Curiae Supporting Neither Party, *Frank v. Gaos*, 584 U.S. __ (2019) (No. 17-961).

The Government's position in this case is inconsistent with its position in *Gaos*. The only support offered for the assertion that Food Marketing Institute has standing to pursue the appeal in this case is the fact that the USDA "had previously given independent assurances that it would not disclose store-level redemption data" and that the agency "affirmatively assured the court that it would not release that data during petitioner's expected appeal." United States *Food Marketing Institute* Amicus, *supra*, at 34. The Government argued that "even though the USDA could have released the data without a court order requiring disclosure," the Petitioners had standing based on a "threatened *injury of disclosure*" because there was a sufficient likelihood that the injury "would be redressed if petitioner prevailed on appeal." *Id.* 35 (emphasis added).

So according to the Government's brief in *Food Marketing Institute*, the disclosure of store purchase data collected by a federal agency can be an injury-in-fact to a trade association even though the trade association was not the one that provided the data to the government and the agency is lawfully permitted to disclose the data. But according to the Government's brief in *Gaos*, the disclosure of an individual's private communications in violation of federal law cannot possibly be an injury-in-fact. That is "pure applesauce." *King v. Burwell*, 135 S. Ct. 2480, 2501 (2015) (Scalia, J., dissenting). And even if a lower court could be convinced that the intervenors in this case have standing to pursue an appeal, that determination cannot be made by the Court in the first instance. *See Gaos*, 584 U.S., slip op. at 6.

CONCLUSION

For the above reasons, EPIC respectfully ask this Court to affirm the decision of the U.S. Court of Appeals for the Eighth Circuit and remand the case.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ENID ZHOU
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

March 25, 2019